IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

JAMES MARLIN, on behalf of himself and all others similarly situated, Plaintiff, v. ASSOCIATED MATERIALS, LLC, Defendant.	Case No. 5:23 CV 1621 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

INTRODUCTION

1. Representative Plaintiff James Marlin ("Representative Plaintiff") brings this class action against Defendant Associated Materials, LLC ("Defendant" or "AM") for its failure to properly secure and safeguard Representative Plaintiff's and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including without limitation, full names, addresses, phone numbers, dates of birth, Social Security numbers and health insurance information (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected health information" or "PHI"[1] and "personally identifiable information" or "PII").[2]

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain

2. With this action, Representative Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiff and numerous other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on May 12, 2023, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PHI/PII which was being kept unprotected (the "Data Breach").

3. Representative Plaintiff further seeks to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

4. While Defendant claims to have discovered the breach as early as May 12, 2023, Defendant did not begin informing victims of the Data Breach until August 8, 2023 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiff and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it. The Notice received by Representative Plaintiff was dated August 8, 2023.

5. Defendant acquired, collected and stored Representative Plaintiff's and Class Members' PHI/PII. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII.

---

identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and insurers, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendant's maintenance of Representative Plaintiff's and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiff's and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

8. By obtaining, collecting, using and deriving a benefit from Representative Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiff does not bring claims in this action for direct violations of HIPAA, but charges Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendant disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and

reasonable measures to ensure that Representative Plaintiff's and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiff's and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiff's claims took place within this District, and Defendant does business in this Judicial District.

PLAINTIFF

14. Representative Plaintiff is an adult individual and, at all relevant times herein, was a resident and citizen of the State of New Jersey. Representative Plaintiff is a victim of the Data Breach.

15. Defendant received highly sensitive PHI/PII from Representative Plaintiff in connection the goods/services/employment Representative Plaintiff obtained/received/requested. As a result, Representative Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

16. At all times herein relevant, Representative Plaintiff is and was a member of the Class.

17. As required in order to obtain services and/or employment from Defendant, Representative Plaintiff provided Defendant with highly sensitive PHI/PII.

18. Representative Plaintiff's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Representative Plaintiff's PHI/PII. Representative Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

19. Representative Plaintiff received a letter from Defendant, dated August 8, 2023, stating Representative Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

20. As a result, Representative Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-

monitoring Representative Plaintiff's accounts and seeking legal counsel regarding Representative Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

21. Representative Plaintiff suffered actual injury in the form of damages to and diminution in the value of Representative Plaintiff's PHI/PII—a form of intangible property that Representative Plaintiff's entrusted to Defendant, which was compromised in and as a result of the Data Breach.

22. Representative Plaintiff suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Representative Plaintiff's PHI/PII.

23. Representative Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft and misuse resulting from Representative Plaintiff's PHI/PII, in combination with Representative Plaintiff's name, being placed in the hands of unauthorized third parties/criminals.

24. Representative Plaintiff has a continuing interest in ensuring that Representative Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

25. Defendant is a Delaware corporation with a principal place of business located at 3773 State Road, Cuyahoga Falls, Ohio 44223. Defendant is an exterior building manufacturer with 11 manufacturing facilities and 130 supply centers across the United States and Canada.[3]

26. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

27. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and the following classes/subclass(es) (collectively, the "Class"):

> **Nationwide Class:**
> "All individuals within the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on May 12, 2023."

28. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards,

---

[3] "*About Us,*" Associated Materials, https://www.associatedmaterials.com/about/ (last accessed August 15, 2023).

sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

29. In the alternative, Representative Plaintiff requests additional subclasses as necessary based on the types of PHI/PII that were compromised.

30. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

31. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believe and, on that basis, alleges that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff's and Class Members' PHI/PII;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' PHI/PII;

11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of the Plaintiff Class in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

32. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

33. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiff.

34. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

35. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

36. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' sensitive data, including but not limited to, full names, addresses, phone numbers,

dates of birth, Social Security numbers and health insurance information. Representative Plaintiff was among the individuals whose data was accessed in the Data Breach.

37. Representative Plaintiff was provided the information detailed above upon Representative Plaintiff's receipt of a letter from Defendant, dated August 8, 2023. Representative Plaintiff was not aware of the Data Breach until receiving that letter.

Defendant's Failed Response to the Breach

38. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiff's and Class Members' PHI/PII.

39. Not until roughly three months after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

40. The Notice included, *inter alia*, the claims that Defendant had learned of the Data Breach on May 12, 2023, and Defendant later discovered the unauthorized access began as early as April 25, 2023.

41. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law and its own assurances and representations to keep Representative Plaintiff's and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

42. Representative Plaintiff and Class Members were required to provide their PHI/PII to Defendant in order to receive services and/or employment, and as part of providing services

and/or employment, Defendant created, collected and stored Representative Plaintiff's and Class Members' PHI/PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

43. Despite this, Representative Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiff and Class Members are thus left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

44. Representative Plaintiff's and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiff's and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiff's and Class Members' PHI/PII.

Defendant Collected/Stored Plaintiff's and Class Members' PHI/PII

45. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiff's and Class Members' PHI/PII.

46. As a condition of its relationships with Representative Plaintiff and Class Members, Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly

sensitive and confidential PHI/PII. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

47. By obtaining, collecting and storing Representative Plaintiff's and Class Members' PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiff's and Class Members' PHI/PII from unauthorized disclosure.

48. Representative Plaintiff and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiff and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

49. Defendant could have prevented the Data Breach, which began no later than April 25, 2023, by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiff's and Class Members' PHI/PII.

50. Defendant's negligence in safeguarding Representative Plaintiff's and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

51. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

52. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiff's and Class Members' PHI/PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

53. In failing to adequately secure Representative Plaintiff's and Class Member's sensitive data, Defendant breached duties it owed Representative Plaintiff and Class Members under statutory and common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' PHI/PII confidential. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiff's and Class Members' PHI/PII. Moreover, Representative Plaintiff and Class Members surrendered their highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII, independent of any statute.

54. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information") and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

55. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

56. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

57. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

58. "Electronic protected health information" is "individually identifiable health information [...] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

59. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

60. HIPAA also requires Defendant to "review and modify the security measures implemented [...] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

61. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

62. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

63. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Representative Plaintiff's and Class Members' PHI/PII.

64. Defendant owed a duty to Representative Plaintiff and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all PHI/PII in its possession was adequately secured and protected.

65. Defendant owed a duty to Representative Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in its

possession, including not sharing information with other entities who maintained substandard data security systems.

66. Defendant owed a duty to Representative Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

67. Defendant owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

68. Defendant owed a duty to Representative Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft, because such an inadequacy would be a material fact in the decision to entrust their PHI/PII to Defendant.

69. Defendant owed a duty of care to Representative Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

70. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt and/or more reliably encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identity possible threats.

Value of the Relevant Sensitive Information

71. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable

commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

72. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

73. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[7] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen or unlawfully disclosed in 505 data breaches.[8] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[9]

74. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain

---

[4] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed August 15, 2023).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed August 15, 2023).

[6] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed August 15, 2023).

[7] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed August 15, 2023).

[8] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed August 15, 2023).

[9] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/ (last accessed August 15, 2023).

PHI/PII compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

75. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

76. Identity thieves can use PHI/PII, such as that of Representative Plaintiff and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

77. The ramifications of Defendant's failure to keep secure Representative Plaintiff's and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiff's and Class Members' PHI/PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

78. There may be a time lag between when harm occurs versus when it is discovered and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

79. The harm to Representative Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[11]

80. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[12]

81. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiff and Class Members.

---

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf/ (last accessed August 15, 2023).
[11] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-identity-theft/ (last accessed August 15, 2023).
[12] *Id.*

82. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[14]

83. And data breaches are preventable.[15] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[16] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised...."[17]

84. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[18]

85. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiff's and Class Members'

---

[13] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed August 15, 2023).
[14] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed August 15, 2023).
[15] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[16] *Id.* at 17.
[17] *Id.* at 28.
[18] *Id.*

PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiff and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

86. Defendant disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff's and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice of the Data Breach.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of the Nationwide Class)

87. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

88. At all times herein relevant, Defendant owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiff's and Class Members' PHI/PII on its computer systems and networks.

89. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession;

b. to protect Representative Plaintiff's and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

90. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

91. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

92. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' PHI/PII.

93. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiff and Class Members had entrusted to it.

94. Defendant breached its duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiff's and Class Members' PHI/PII.

95. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained thereon.

96. Representative Plaintiff's and Class Members' willingness to entrust Defendant with its PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII it stored on them from attack. Thus, Defendant had a special relationship with Representative Plaintiff and Class Members.

97. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiff and/or the remaining Class Members.

98. Defendant breached its general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiff's and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiff's and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

99. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

100. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

101. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

102. Defendant breached its duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting roughly three months after learning of the Data Breach to notify Representative Plaintiff and Class Members and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

103. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiff and Class Members, Defendant prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their PHI/PII.

104. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiff's and Class Members' PHI/PII and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiff and Class Members. Representative Plaintiff's and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

105. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

106. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

107. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair [...] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

108. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

109. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se.* Defendant also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

110. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

111. As a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

112. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession

and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Nationwide Class)

113. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

114. Through their course of conduct, Defendant, Representative Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PHI/PII.

115. Defendant required Representative Plaintiff and Class Members to provide and entrust their PHI/PII as a condition of obtaining Defendant's goods/services/employment from/with Defendant.

116. Defendant solicited and invited Representative Plaintiff and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiff and Class Members accepted Defendant's offers and provided their PHI/PII to Defendant.

117. As a condition of being direct customers and/or employees of Defendant, Representative Plaintiff and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiff and Class Members if its data had been breached and compromised or stolen.

118. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

119. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

120. Defendant breached the implied contracts it made with Representative Plaintiff and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

121. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Nationwide Class)

122. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth therein.

123. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

124. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

125. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiff and Class Members and continued acceptance of PHI/PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

126. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

RELIEF SOUGHT

WHEREFORE, Representative Plaintiff, on Representative Plaintiff's own behalf and on behalf of each member of the proposed National Class, respectfully requests that the Court enter judgment in favor of Representative Plaintiff and the Class and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class and/or any other appropriate Subclasses under Federal Rules of Civil Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiff and Class Members;

5. For injunctive relief requested by Representative Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

c. requiring Defendant to delete and purge Representative Plaintiff's and Class Members' PHI/PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the

employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Class and/or Subclasses, hereby demands a trial by jury for all issues triable by jury.

Dated: August 15, 2023

Respectfully submitted,

By: _____

Elizabeth Ruth Klos, Esq. (C.A. S.B. #346781)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: erk@colevannote.com

Attorneys for Representative Plaintiff and the Plaintiff Classes

**Pro hac vice forthcoming*